## CLAIMS

What is claimed is:

1. A settop terminal in a subscriber television system, the settop terminal comprising:

a first memory having an encrypted first key and an encrypted device key set stored therein;

a secure element having a processor and a second memory, wherein the second memory is accessible only to the processor and has a private-key of a private-key/public-key pair stored therein, wherein the processor is adapted to decrypt the encrypted first key using the private-key, and wherein the decrypted first key is used to decrypt the encrypted device key set; and

an adaptive output interface adapted to utilize a device key set to determine a shared-secret key with a receiver in communication therewith and adapted to provide an encrypted stream of content to the receiver using the shared-secret key to encrypt the stream of content.

2. The settop terminal of claim 1, wherein the device key set is used with protocols for high-bandwidth digital content protection.

3. The settop terminal of claim 1, wherein the device key set is used with protocols for digital transmission content protection.

4. The settop terminal of claim 1, wherein the adaptive output interface includes at least one of a digital visual interface and a High-Definition Multimedia Interface [HDMI].

5. The settop terminal of claim 1, wherein the output interface includes an IEEE 1394 interface.

6. The settop terminal of claim 1, further including:

a second processor adapted to receive the decrypted first key and decrypt the encrypted device key set using the decrypted first key and provide the decrypted device key set to the adaptive output interface.

7. The settop terminal of claim 6, wherein second processor implements a symmetric cryptographic algorithm using the device-key set decryptor as a key to decrypt the encrypted device-key set.

8. The settop terminal of claim 7, wherein the symmetric cryptographic algorithm is a 3DES algorithm.

9. The settop terminal of claim 7, wherein the symmetric cryptographic algorithm is a DES algorithm.

10. The settop terminal of claim 1, wherein the encrypted device key set and the encrypted first key are stored in the first memory prior to installing the settop terminal in the subscriber television system.

11. In a subscriber television system having a headend in communication with a plurality of settop terminals including a given settop terminal, the given settop terminal comprising:

a first memory having an encrypted first key and an encrypted device key set stored therein;

a secure element having a first processor and a second memory, wherein the second memory is accessible only to the first processor and has a private-key of a private-key/public-key pair stored therein, wherein the first processor is adapted to decrypt the encrypted first key using the private-key;

an input port receiving a stream of content from the headend;

a second processor adapted to determine from the stream of content whether the content of the stream of content is protected and adapted to receive the decrypted first key and decrypt the encrypted device key set using the decrypted first key; and

an adaptive output interface adapted to implement the decrypted device key set to determine a shared-secret key with a receiver in communication therewith and, responsive to the first processor determining the content is protected, adapted to provide an encrypted stream of content to the receiver using the shared-secret key to encrypt the stream of content, and, responsive to the first processor determining the content is not protected, adapted to provide the stream of content to the receiver;

12. The settop terminal of claim 11, wherein the device key set includes protocols for high-bandwidth digital content protection.

13. The settop terminal of claim 11, wherein device key set includes protocols for digital transmission content protection.

14. The settop terminal of claim 11, wherein the adaptive output interface includes at least one of a digital visual interface and a High-Definition Multimedia Interface [HDMI].

15. The settop terminal of claim 11, wherein the output interface includes an IEEE 1394 interface.

16. A method of providing a receiver with a stream of content, the method implemented in a settop terminal in a subscriber television system, the method comprising the steps of:

decrypting an encrypted first key using a private-key of a private-key/public-key pair belonging to the settop terminal, wherein the first key is decrypted inside of a secure-element having a processor and a memory, wherein the private-key is accessible to only the processor;

decrypting an encrypted device key set using the decrypted first key;

providing the decrypted device key set to an adaptive output interface;

determining a shared-secret key with the receiver using the decrypted device key set; and

outputting the stream of content to the receiver.

17. The method of claim 16, prior to the step of outputting, further including the steps of:

determining whether the content of the stream of content is protected content; and

responsive to determining the content is protected, encrypting the content of the stream of content using the shared-secret key, wherein the output stream of content is encrypted.

18. The method of claim 17, prior to the step of encrypting the content, further including the steps of:

receiving a second encrypted stream of content; and

decrypting the second stream of content, wherein the decrypted second stream of content is the stream of content that is encrypted in the encryption step.

19. A method of providing a receiver with a stream of content, the method implemented in a settop terminal in a subscriber television system, the method comprising the steps of:

decrypting an encrypted first key using a private-key of a private-key/public-key pair belonging to the settop terminal, wherein the first key is decrypted inside of a secure-element having a processor and a memory, wherein the memory is accessible to only the processor and has the private-key stored therein;

decrypting an encrypted device key set using the decrypted first key;

providing the decrypted device key set to an adaptive output interface;

negotiating a shared-secret key with the receiver using the decrypted device key set;

receiving a stream of content from a headend of the subscriber television system;

determining whether the receiver is entitled to access the stream of content;

determining whether the received stream of content is encrypted content; and

outputting the stream of content to the receiver.

20. The method of claim 16, prior to the step of outputting, further including the steps of:

determining whether the content of the stream of content is protected content; and responsive to determining the content is protected, encrypting the content of the stream of content using the shared-secret key, wherein the output stream of content is encrypted.